UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,693	03/08/2006	Bernard Le Bars	274883US2PCT	3914

22850 7590 12/28/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
ARMOUCHE, HADI S	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
12/28/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/541,693	**Applicant(s)** LE BARS ET AL.	
	Examiner HADI ARMOUCHE	**Art Unit** 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 October 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to applicant's amendment filed on 09/10/2009. Claims 11, 13-14, 18 and 21 have been amended. Claims 11-21 remain pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/09/2009 has been entered.

Response to Arguments

3. Applicant's arguments (page 7 of the remarks) filed on 09/10/2009, with respect to the rejection of claim 11 under 35 USC 112, second paragraph, have been fully considered and are persuasive. The rejection of claim 11 under 35 USC 112 has been withdrawn.

4. It has been argued (pages 8-13) that Moroney and the other cited references don't teach the newly added limitations.

5. Applicant's interpretation of the reference is noted. However, examiner respectfully disagrees. Moroney in paragraph 0031 teaches:

> Each set-top is equipped with two cryptographic keys: a unit key and an authentication key. The unit key is used for reconfiguration, and the authentication key is shared between a master-slave pair to verify that they have not been separated. Both keys are delivered to the set-tops in encrypted form,

> so that neither the installer, customer, nor authorized agent is aware of the true key values. The initial ("provisioning") keys are provided during the manufacturing process of the set-tops.

In paragraphs 0037 and 155, Moroney teaches that the keys are biunique (same, symmetric, identical)

> Since a master-slave pair share the same authentication key which is unknown outside of the two set-tops and the billing software, it has the necessary cryptographic values to verify that the two set-tops are linked together.

> Although this protocol has been described using entirely symmetric key cryptography ...

Later in paragraph 0037, Moroney teaches:

> The master does a cryptographic signature of the received value via a message authentication code (MAC) using the shared authentication key, and sends the result back to the slave. The slave verifies that the correct signature was obtained, including the use of the correct pseudo-randomly generated value sent, and if so, continues operation as normal. If the slave did not receive the correct response or did not receive any response within some fixed time interval, the slave repeats its request up to some fixed number of times. If it still fails to receive the correct reply, it then discontinues displaying cable/satellite television until the master gives the correct reply.

Therefore, if the key in the slave is the same as the key in the master, then the service is discontinued. Otherwise, the operation continues as normal.

6. Applicant is encouraged to schedule an interview with the examiner prior to the next communication.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

8. Claims 11 and 21 are rejected under 35 U.S.C. 102(a) as being anticipated by Moroney et al. (US 2003/0097563) referred to hereinafter by Moroney.

9. Regarding claim 11, Moroney teaches *a method for distribution of scrambled data and/or services to at least one master terminal and to at least one slave terminal linked with the master terminal, the method comprising: transmitting by a central management module to the master terminal a first secret code S_m and transmitting by the central management module to each slave terminal a second secret code S_s; storing the first secret code S_m in the master terminal and the second secret code Ss in each slave terminal and, for each use of a slave terminal by a user, checking whether the first secret code S_m has previously been stored in the slave terminal, when the first secret code S_m has previously been stored in the slave terminal, checking whether the first secret code S_m is in a biunique relationship with the second secret code S_s when the first secret code S_m has not previously been stored in the slave terminal, inviting said user to enter the first secret code S_m in said slave terminal, and checking whether the first secret code S_m entered by the user in the slave terminal is in a biunique relationship with the second secret code S_s authorizing the reception of the scrambled data and/or*

services by the slave terminal, when the first secret code S_m is in a biunique relationship with the second secret code S_s and prohibiting the reception of the scrambled data and/or services by the slave terminal, when the first secret code S_m is not in a biunique relationship with the second secret code S_s [paragraphs 19-23, 31, 36-38, 58, 63 and 155 teaches installing an identical/symmetric keys (biunique) in both the master and the slave set-top boxes) by a central authorized agent. Upon communication if the keys don't match, then the service is discontinued; otherwise, service is provided to the slave device].

10. Regarding claim 21, Moroney teaches that *the slave terminal is not authorized to be used by said user when said first secret code S_m is not already stored in the slave terminal or when said second secret code Ss is not in a biunique relationship with the secret code S_m previously saved in the slave terminal* [paragraphs 19-23, 31, 36-38, 58, 63 and 155].

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moroney in view of Okimoto et al. (US 2002/0051359) referred to hereinafter by Okimoto.

13. Regarding claim 12, Moroney does not disclose a system in which the codes are distributed inside of EMMs that are sent to each individual terminal. The step of sending an EMM to each individual terminal is shown in (Okimoto [0010], [0011]). It would have been obvious to one of ordinary skill in the art at the time of invention to modify Moroney to deliver an EMM to each terminal, as taught by Okimoto, so that each terminal contains individual rights and privileges and cannot be used to intercept the signals being sent to other terminals.

14. Regarding claim 13, Moroney teaches *transmitting by the central management module to the master terminal the new first secret code and to each slave terminal the new second secret code; storing the new first secret code in the master terminal and the new second secret code in each slave terminal and, for each use of the slave terminal by the user, checking whether the new first secret code has previously been stored in the slave terminal, when the new first secret code has previously been stored in the slave terminal, checking whether the new first secret code is in a biunique relationship with the new second secret code, when the new first secret code has not previously been stored in the slave terminal, inviting the user to enter the new first secret code in the slave terminal, and checking whether the new first secret code entered by the user in the slave terminal is in a biunique relationship with the new second secret code, authorizing the reception of the scrambled data and/or services by the slave terminal, when the new first secret code is in a biunique relationship with the new second secret code, and prohibiting the reception of the scrambled data and/or services by the slave*

terminal, when the new first secret code is not in a biunique relationship with the new second secret code [paragraphs 19-23, 31, 36-38, 58, 63 and 155].

However, Moroney does not teach *generating at a variable frequency a new first secret code and a new second secret code.* The step of generating new codes at variable frequencies is shown in (Okimoto [0013]), which teaches a system in which terminals will periodically receive renewed keys that are necessary for the decryption of broadcast data. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Moroney to periodically renew decryption keys, as taught by Okimoto, in order to stop compromised keys from being valid for extended periods of time.

15. Regarding claim 14, the steps of transmitting and storing data are shown in (Moroney [0019]-[0023], [0031], [0036], and [0037]), which teaches a system in which both the master and slave boxes must be delivered identical authentication keys. The slave will not decode the material if the authentication keys are not correct. Moreover, Moroney as explained earlier in claims 11 and 13 teaches that *for each use of the slave terminal, checking whether the new first secret code has previously been stored in the slave terminal, when the new first secret code has previously been stored in the slave terminal, checking whether the new first secret code is in a biunique relationship with the new second secret code, when the new first secret has not previously been stored in the slave terminal, inviting the user to enter the first secret code in the slave terminal, and checking whether the new first secret code entered by the user in the slave terminal is in a biunique relationship with the new second secret code, authorizing the reception*

of the scrambled data and/or services by the slave terminal, when the new first secret code is in a biunique relationship with the new second secret code, and prohibiting the reception of the scrambled data and/or services by the slave terminal, when the new first secret code is not in a biunique relationship with the new second secret code [paragraphs 19-23, 31, 36-38, 58, 63 and 155].

Moroney does not disclose a system in which the codes are distributed inside of EMMs that are sent to each individual terminal. The step of sending an EMM to each individual terminal is shown in (Okimoto [0010], [0011]). It would have been obvious to one of ordinary skill in the art at the time of invention to modify Moroney to deliver an EMM to each terminal, as taught by Okimoto, so that each terminal contains individual rights and privileges and cannot be used to intercept the signals being sent to other terminals.

16. Claims 15-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moroney, in view of Le Berre et al. (US 5,748,732), hereafter referred to as Le Berre.

17. Regarding claim 15: Moroney does not disclose a system where both a master and slave terminals contain security processors.

A system in which both the master and slave terminals contain security processors is shown in (Le Berre, column 1, line 62 to column 2, line 22).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Moroney to include security processors in both the master and slave ends of the communications, as taught by Le Berre, in order to prevent malicious messages from being created, distributed, or accepted by the master or slave terminals.

18. Regarding claim 16: Moroney does not disclose a system in which security processors are linked to smart cards.

A system in which security processors are linked to smart cards is shown in (Le Berre column 2, lines 5-22), which teaches that the security processors of both the master and slave card use smart cards.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Moroney to link smart cards with the terminals, as taught by Le Berre, in order to provide strong authentication in a flexible, secure, standard way with minimal human intervention.

19. Regarding claim 17: Moroney does not disclose a system in which smart cards are paired with individual terminals.

A system that uses smart cards paired with individual terminals is disclosed in (Le Berre column 4, lines 24-31), which teaches a system in which each smart card is uniquely paired with its respective terminal.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Moroney to pair smart cards with terminals, as taught by Le Berre, in order to prevent smart cards being moved from a valid receiver to a stolen, illicit, or non-privileged receiver.

20. The rejection of claim 18 is similar to that of claim 11. Additional limitation includes a central subscriber management module. Moroney does not disclose a central subscriber management module, an EMM generator, and a scrambling platform.

A system that contains a central subscriber management module, an EMM generator, and a scrambling platform (Le Berre column 1, line 62 to column 2, line 4), which teaches a system with a central management device that generates and encrypts entitlement management messages.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Moroney to generate and encrypt EMMs at a central source, as taught by Le Berre, in order to distribute corresponding EMMs to the correct terminals and prevent other terminals from intercepting or decrypting content not intended for them.

21. Regarding claim 19, A system in which a single master terminal is paired with a single slave terminal is shown in (Moroney [0018]), which shows a master decoder attached to at least one slave decoder.

22. Regarding claim 20, *a system according to claim 18, comprising a plurality of master terminals and a plurality of slave terminals*. Both Moroney and Le Berre disclose a single master and multiple slave terminals for one user. If a plurality of users exists, there would be multiple master and multiple slave terminals.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432